AMENDMENTS TO THE CLAIMS:

1-8. (Cancelled)

9. (Previously presented) A method to automatically handle undesired electronic mail (e-mail) in communication networks at the receiver, the method comprising:

automatically comparing the sender address accompanying an incoming e-mail to an electronically accessed list of authorized sender addresses assigned to the receiver; and then

storing the e-mail in a mailbox MB of the recipient, wherein the only e-mails transferred to the receiver's mailbox are those that had clearly been sent by authorized senders;

in combination with:

performing an analysis to see if there is serial, incremental user identification occurring so that conclusions can be drawn concerning automatic attempts at breaking into the e-mail system.

10. (Previously presented) The method according to claim 9, wherein there are two logically or physically, or both, separate mailboxes, said mailbox MB and a junk mailbox JMB, wherein the e-mail server sends to the JMB mailbox all incoming e-mails that indeed have the subscriber's correct recipient address but are not contained in the sender list on the receiving side, thus making them available for further processing selectively by the internet service provider, the administrative authorities, and by the recipient.

11. (Previously presented) The method according to claim 9, wherein the incoming e-mails are selectively put through an automatic handling and analysis process, which can be selectively configured by the recipient and by the ISP, selectively in the e-mail server, in a comparison device, and in at least one of the mailboxes, said process initiated and configured either on a case-by-case basis or permanently.

12. (Previously presented) The method according to claim 10, wherein the incoming e-mails are selectively put through an automatic handling and analysis process, which can be selectively configured by the recipient and by the ISP, selectively in the e-mail server , in a comparison device, and in at least one of the mailboxes, said process initiated and configured either on a case-by-case basis or permanently.

13. (Currently amended) The method according to claim 9, wherein ~~all~~ when executable programs are sent as attachments to e-mails, all said executable programs are automatically separated in the JMB.

14. (Currently amended) The method according to claim 10, wherein ~~all~~ when executable programs are sent as attachments to e-mails, all said executable programs are automatically separated in the JMB.

15. (Currently amended) The method according to claim 11, wherein ~~all~~ when executable programs are sent as attachments to e-mails, all said executable programs are automatically separated in the JMB.

16. (Currently amended) The method according to claim 12, wherein ~~all~~ when executable programs are sent as attachments to e-mails, all said executable programs are automatically separated in the JMB.

17. (Previously presented) The method according to claim 9, wherein if an undesired e-mail is received, discontinuation requests, or cease and desist demands, can be generated automatically and delivered to the sender.

18-20. (Cancelled)

21. (Previously presented) The method according to claim 9, wherein virus checks of the e-mail can be carried out selectively at an established time of day or each time a message arrives.

22-24. (Cancelled)

25. (Previously presented) The method according to claim 10, wherein the contents of the JMB can be cyclically deleted at specific time intervals.

26-28. Cancelled

29. (New) A method to automatically handle undesired electronic mail (e-mail) in communication networks at the receiver, the method comprising:

automatically comparing the sender address accompanying an incoming e-mail to an electronically accessed list of authorized sender addresses assigned to the receiver; and then

storing the e-mail in a mailbox MB of the recipient, wherein the only e-mails transferred to the receiver's mailbox are those that had clearly been sent by authorized senders;

in combination with:

performing an analysis to see if there is serial, incremental user identification occurring, which would enable inferences to be drawn concerning automatic attempts at breaking into the e-mail system that automatically try all possible codes.

30. (New) The method according to claim 29, wherein when executable programs are sent as attachments to e-mails, all said executable programs are automatically separated in the JMB.

31. (New) The method according to claim 29, wherein if an undesired e-mail is received, discontinuation requests, or cease and desist demands, can be generated automatically and delivered to the sender.

32. (New) The method according to claim 29, wherein virus checks of the e-mail can be carried out selectively at an established time of day or each time a message arrives.

33. (New) The method according to claim 29, wherein the contents of the JMB can be cyclically deleted at specific time intervals.

34. (New) A method to automatically handle undesired electronic mail (e-mail) in communication networks at the receiver, the method comprising:

automatically comparing the sender address accompanying an incoming e-mail to an electronically accessed list of authorized sender addresses assigned to the receiver; and then

storing the e-mail in a mailbox MB of the recipient, wherein the only e-mails transferred to the receiver's mailbox are those that had clearly been sent by authorized senders;

in combination with:

performing an analysis to see if a serial, incremental change in user identification is occurring so that conclusions can be drawn concerning automatic attempts at breaking into the e-mail system by automatically, serially, incrementally changing the user identification until the changed user identification matches an authorized user identification.

35. (New) The method according to claim 34, wherein when executable programs are sent as attachments to e-mails, all said executable programs are automatically separated in the JMB.

36. (New) The method according to claim 34, wherein if an undesired e-mail is received, discontinuation requests, or cease and desist demands, can be generated automatically and delivered to the sender.

37. (New) The method according to claim 34, wherein virus checks of the e-mail can be carried out selectively at an established time of day or each time a message arrives.